IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

DEMOCRATIC NATIONAL COMMITTEE
and DEMOCRATIC PARTY OF WISCONSIN,

Plaintiffs,

v. Case No. 20-cv-249-wmc

MARGE BOSTELMANN, JULIE M. GLANCEY, ANN S. JACOBS, DEAN KNUDSON, ROBERT F. SPINDELL, JR. and MARK L. THOMSEN,

Defendants,

and

REPUBLICAN NATIONAL COMMITTEE
and REPUBLICAN PARTY OF WISCONSIN,

Intervening Defendants.

SYLVIA GEAR, CLAIRE WHELAN, WISCONSIN ALLIANCE FOR RETIRED AMERICANS, LEAGUE OF WOMEN VOTERS OF WISCONSIN, KATHERINE KOHLBECK, DIANE FERGOT, GARY FERGOT, BONIBET BAHR OLSAN, SHEILA JOZWIK, and GREGG JOZWIK,

Plaintiffs,

v. Case No. 20-cv-278-wmc

MARGE BOSTELMANN, JULIE M. GLANCEY, ANN S. JACOBS, DEAN KNUDSON, ROBERT F. SPINDELL, JR., MARK L. THOMSEN, and MEAGAN WOLFE,

Defendants.

CHRYSTAL EDWARDS, TERRON EDWARDS, JOHN JACOBSON, CATHERINE COOPER, KILEIGH HANNAH,

KRISTOPHER ROWE, KATIE ROWE, CHARLES DENNERT, JEAN ACKERMAN, WILLIAM LASKE, JAN GRAVELINE, TODD GRAVELINE, ANGELA WEST, DOUGLAS WEST, and all others similarly situated,

Plaintiffs,

v. Case No. 20-cv-340-wmc

ROBIN VOS, SCOTT FITZGERALD, WISCONSIN STATE ASSEMBLY, WISCONSIN STATE SENATE, WISCONSIN ELECTIONS COMMISSION, MARGE BOSTELMANN, JULIE M. GLANCEY, ANN S. JACOBS, DEAN KNUDSON, ROBERT F. SPINDELL, JR., MARK L. THOMSEN, and MEAGAN WOLFE,

Defendants.

JILL SWENSON, MELODY McCURTIS, MARIA NELSON, BLACK LEADERS ORGANIZING FOR COMMUNITIES, DISABILITY RIGHTS WISCONSIN

Plaintiffs,

v. Case No. 20-cv-459-wmc

MARGE BOSTELMANN, JULIE M. GLANCEY, ANN S. JACOBS, DEAN KNUDSON, ROBERT F. SPINDELL, JR., MARK L. THOMSEN, and MEAGAN WOLFE,

Defendants.

DECLARATION OF MATTHEW BERNHARD

---

1. I am a Ph.D. candidate at the University of Michigan in Computer Science with a focus on computer security. I received my Bachelor's degree from Rice University, and my Master's in Computer Science from the University of Michigan.
2. I have focused my study in the field of computer science, including cyber-security in voting systems since 2012, including specific work on new, secure voting technology (the STAR-Vote system from Austin, Texas). I have worked with the Verified Voting Foundation on gathering data about currently deployed voting systems. I consulted with a political candidate's campaign in 2016 to assess threat models and incident reports in Michigan, Wisconsin, and Pennsylvania. I have worked with other experts in the field to provide a theoretical survey of properties of election security and served as an expert witness in voting related cases in the state of Georgia (*Coalition for Good Governance, et al. v. Crittenden et al.,* 2018CV31348) and federal court *(Curling, et al. v. Raffensperger, et al.* 1:17-cv-2989-AT, *Shelby Advocates for Valid Elections, et al., v. Hargett, et al.* **No.** 2:18-cv-02706). I have produced award-winning research about election systems and their security.
3. I have published and spoken extensively about cybersecurity and other risks of electronic voting systems and have assisted in preparation of other experts for Congressional testimony concerning these topics. I have testified before the U.S. Commission on Civil Rights about the security realities of voting in the United States.
4. A copy of my curriculum vitae is attached as Exhibit A.

The relief proposed by the *Gear* Plaintiffs is secure.

5. The *Gear* Plaintiffs have asked me to review their proposed relief for their claims challenging the failure to deliver absentee ballots and to evaluate the security implications

of enabling domestic Wisconsin voters to request replacement ballots via the online portal myvote.wi.gov (hereinafter "MyVote").

6. I have reviewed the plaintiff's proposal in their First Amended Complaint and their preliminary injunction motion, and it is my opinion that said proposal does not pose a security risk to voters in Wisconsin. The scope of the relief is narrow and will only affect voters who do not receive their absentee ballot in time to cast it in the election.

7. I have reviewed the Wisconsin Election Commission ("WEC") report on the absentee voting delivery issues for the April 7th election,[1] as well as portions of the deposition transcript from Meagan Wolfe's July 3, 2020 deposition, the declarations submitted by current and former municipal clerks Tara Coolidge, Maribeth Witzel-Behl, and Debra Salas, as well as the MyVote manual.[2]

8. Based on the testimony of clerks in Wisconsin, my understanding of the MyVote process for downloading an absentee ballot, and my expertise in the field of cybersecurity and election security, it is my opinion that Plaintiffs' proposed remediation does not pose any additional security risk to Wisconsin elections.

9. This opinion is based on four facts: (1) the subset of voters who will have access to the proposed relief is limited; (2) the voters who can use the proposed relief will have been authenticated already and will also have to authenticate to MyVote using additional credentials; (3) the WEC has robust, defense-in-depth procedures for preventing fraud in

[1] Wisconsin Elections Commission, April 7, 2020 Absentee Voting Report ("Post-Election Absentee Voting Report") (May 15, 2020), https://elections.wi.gov/sites/elections.wi.gov/files/2020-05/April%202020%20Absentee%20Voting%20Report.pdf.

[2] Wisconsin Elections Commission, MyVote Wisconsin: A Guide to the MyVote Wisconsin Website for Voters and Clerks, at 20-21, https://elections.wi.gov/sites/elections.wi.gov/files/publication/65/myvote_manual_sept_2016_pdf_21316.pdf.

absentee ballots; and (4) fraud in elections in the United States and in Wisconsin in particular is so rare as to be functionally non-existent.

Access to MyVote ballot downloads will be highly restricted.

10. Voters who gain the ability to download a ballot through MyVote will only be able to do so if they have previously requested and not received an absentee ballot via mail, and only if they do so within a specified window of time. Limiting the use of MyVote's mail-in absentee ballot portal in this way is a well-established security practice in election security literature.[3,4]

11. While there is no evidence that voter ID requirements have an impact on the prevention of voter fraud,[5] voters who will use MyVote to access a replacement absentee ballot will have already met the voter ID requirements in Wisconsin. These voters will thus have reached a higher bar of authentication than military and overseas voters, who are exempt from the photo identification verification requirement.

12. The MyVote portal already uses standard identity authentication information by requiring the voter input their name, date of birth, and the last four digits of their Social Security Numbers[6] (which have been established as the most secure part of SSNs by Acquisti and Gross).[7]

---

[3] Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?." In *41st IEEE Symposium on Security and Privacy*. 2020.

[4] Appel, Andrew W., Richard A. DeMillo, and Philip B. Stark. "Ballot-Marking Devices Cannot Ensure the Will of the Voters." *Election Law Journal: Rules, Politics, and Policy* (2020).

[5] Cantoni, Enrico, and Vincent Pons. *Strict ID Laws Don't Stop Voters: Evidence from a US Nationwide Panel, 2008–2016*. No. w25522. National Bureau of Economic Research, 2019.

[6] Wolfe Tr. at 156:16-157:2

[7] Acquisti, Alessandro, and Ralph Gross. "Predicting social security numbers from public data." *Proceedings of the National Academy of Sciences* 106, no. 27 (2009): 10975-10980.

13. Plaintiffs' proposed relief would not consist of substantive changes to the existing workflow of the MyVote ballot retrieval process. As voters' photo IDs will have already been verified by their clerk and input in MyVote, the MyVote page only needs to make one transaction with personally identifiable information (PII), in which voters request a replacement ballot through the MyVote page in the same way that military and overseas voters currently do. The MyVote page would then have to confirm that a photo ID verification had already taken place, which it can do in the same check it performs on the voter's name, date of birth, and the last 4 digits of their SSN, and then build and send a ballot back to the voter. This should only require one transaction of PII, not two as indicated by Administrator Meagan Wolfe in her deposition. 20-cv-249, dkt. 247, Wolfe Tr. 155:18-21.

14. Since the proposed relief would require only one transaction with personally identifiable information (PII), it will be functionally the same as the existing workflow, which is acknowledged by the WEC Administrator as secure: "[T]here's only, you know, one point of that data exchange, right, for them because there isn't that intermediary step but, yes, we – we consider it to be very secure[9]

15. The MyVote portal prohibits the ability to download the ballot more than three times.[10] While this does not preclude the ability to copy the ballot once downloaded, it is a robust safeguard that balances the voter's right to ballot access against the risk of any security breach, however remote or unlikely to affect the election.

---

[9] Wolfe Tr. 157:6-9.
[10] MyVote Manual, page 21.

16. Voters' requests to use the portal will also result in their clerk cancelling their existing mail ballot request, eliminating the possibility that a voter can have multiple live ballots issued at once, and therefore eliminating any opportunity for double voting.

17. That access to the portal for replacement ballots could be further limited in time restricts the access to the system even more. It is unlikely that actors seeking to commit fraud would be able to take advantage of the MyVote portal, for the aforementioned reasons, but also because a week is not enough time to fraudulently access and submit a substantial number of fraudulent ballots.

Voter fraud in the United States is practically non-existent.

18. Voter fraud is exceedingly rare. Existing literature has found fewer than 100 fraudulently cast votes (where a voter has submitted a ballot that was not theirs) over the past twenty years of elections in the United States. Over that time, billions of ballots were cast, making the rate of fraud vanishingly small.[11,12]

19. I have reviewed the deposition of Administrator Meagan Wolfe, in which she indicated that she has no knowledge of anyone committing fraud using the MyVote portal in its capacity to facilitate online ballot delivery.[13]

Wisconsin's absentee balloting process has defense in depth.

20. Another significant mitigation to the risk of fraud against this system is that it still ultimately relies on paper ballots sent through physical mail, to date one of the most secure and verifiable election schemes as noted by the National Academies of Science,

---

11 https://www.brennancenter.org/sites/default/files/analysis/Briefing_Memo_Debunking_Voter_Fraud_Myth.pdf

12 Schultz, David. "Less than fundamental: The myth of voter fraud and the coming of the second great disenfranchisement." *Wm. Mitchell L. Rev.* 34 (2007): 483.

13 Wolfe Tr. at 160:17-161:4.

Engineering, and Medicine.[14] This elides potential security issues with online ballot marking, as reported by Specter et al.[15] and Specter and Halderman.[16] That voters can print out and hand-mark their ballots also mitigates issues with ballot marking, as noted in Bernhard et al.,[17] Appel et al.,[18] and Kortum et al.[19]

21. An attacker seeking to commit fraud using the proposed relief would have to ascertain that the voter has requested an absentee ballot, hope that the voter does not receive or mail their actual ballot in time, correctly guess the voter's login credentials, send the ballot from an unsuspicious address, and provide a voter signature that does not arouse suspicion.

22. An attacker who could overcome those significant burdens of fraudulently requesting online ballot delivery would still not be able to scale an attack to more than a small number of voters, because of the difficulty of pulling off the attack for even one voter and the limited amount of time available with which to mount such an attack.

23. Moreover, the more votes an attacker tries to cast fraudulently, the more likely it is they will be detected. Acquisti demonstrated that it would require at least 20 attempts for an attacker to correctly guess the last four digits of just one SSN, with the median requiring thousands of attempts.[20] If the attacker was making these attempts on the MyVote page,

---

[14] National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*. National Academies Press, 2018.
[15] Specter, Michael A., James Koppel, and D. Weitnzer. "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections." *Preprint available at: https://internetpolicy. mit. edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public. pdf* (2020).
[16] Specter, Michael A., and J. Alex Halderman. "Security Analysis of the Democracy Live Online Voting System." (2020).
[17] See footnote 3.
[18] See footnote 4.
[19] Kortum, Philip, Michael D. Byrne, and Julie Whitmore. "Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't." *arXiv preprint arXiv:2003.04997* (2020).
[20] See footnote 6.

their web traffic would be easily identifiable as fraud. Moreover, as absentee ballots for the voters we are discussing will be sent largely to addresses within Wisconsin, an attacker will find it difficult to send ballots from enough addresses the not arouse suspicion. Moreover, the voters the attacker is trying to cast votes in place of are also likely to notice that they have not received their ballots. Of note, it is for exactly this reason that one of the largest and most recent cases of voter fraud was detected and prevented: voters notifying their clerk that they did not receive their ballot, or that someone attempted to cast it for them.[21]

24. Because of the many layered defenses the WEC already has in place on absentee voting and online ballot delivery, a concept known as defense in depth, the already vanishingly small likelihood of fraud is all but completely eliminated. To quote from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA):

> Layering security defenses in an application can reduce the chance of a successful attack. Incorporating redundant security mechanisms requires an attacker to circumvent each mechanism to gain access to a digital asset. For example, a software system with authentication checks may prevent an attacker that has subverted a firewall. Defending an application with multiple layers can prevent a single point of failure that compromises the security of the application.[22]

25. To summarize, because the pool of voters who will be eligible to receive their ballots through MyVote will be limited, said pool of voters will have already had their identities verified by their clerk, the window of time in which voters can access MyVote to request a replacement ballot is short, because fraud is known to be practically non-existent, and because Wisconsin has significant defense-in-depth measures to prevent fraud and other

[21] https://www.npr.org/2019/07/30/746800630/north-carolina-gop-operative-faces-new-felony-charges-that-allege-ballot-fraud
[22] https://us-cert.cisa.gov/bsi/articles/knowledge/principles/defense-in-depth

attacks, extending the usage of the MyVote portal to domestic civilian voters who do not receive their mail-in ballot in time to cast it in the November election does not pose a risk to the integrity of that election.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 8th day of July, 2020.

s/Matthew Bernhard

EXHIBIT A

Matthew Bernhard

Ph.D. Candidate,
Computer Science and Engineering
University of Michigan

2260 Hayward Street
Ann Arbor, MI 48109 USA
matber@umich.edu

mbernhard.com

July 8, 2020

Research Overview

My research focuses on areas where the security and privacy implications of sophisticated systems impacts users in the real world. My interests include election security, usability, human-computer interaction, censorship measurement and resistance, Internet measurement, cryptography, statistics, and systems security. I'm also interested in the intersection of computer science, psychology, politics, and policy.

Education

- Ph.D in Computer Science, University of Michigan, Expected July 2020
  Election Security is Harder Than You Think
  Advisor: J. Alex Halderman
  Committee: Nikola Banovic, Peter Honeyman, Walter R. Mebane, Jr., Ronald L. Rivest
- M.S. in Computer Science, University of Michigan, Summer 2018
- B.A. in Computer Science, Rice University, Spring 2015
  Advisor: Dan S. Wallach

Refereed Conference Publications

[1] **Can Voters Detect Malicious Manipulation of Ballot Marking Devices?**
Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman
In *Proceedings of the 41st IEEE Symposium on Security and Privacy*
(Oakland'20) , May 2020.
Best Student Paper Award

[2] **Decentralized Control: A Case Study of Russia**
Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi
In *Proceedings of the 27th Network and Distributed Systems Symposium*
(NDSS'20) , February 2020.

[3] **UnclearBallot: Automated Ballot Image Manipulation**
Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman
In *Proceedings of the 4th International Joint Conference on Electronic Voting*
(E-Vote-ID'19) , October 2019.

[4] **On the Usability of HTTPS Deployment**
Matthew Bernhard, Jonathan Sharman, Claudia Ziegler Acemyan, Philip Kortum, Dan S. Wallach, and J. Alex Halderman
In *Proceedings of the ACM Conference on Human Factors on Computing Systems* **(CHI'19)** , May 2019.

[5] **403 Forbidden: A Global View of CDN Geoblocking**
Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, Roya Ensafi
In *Proceedings of the ACM Internet Measurement Conference* **(IMC'18)** , November 2018.

[6] **Public Evidence from Secret Ballots**
Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach
In *Proceedings of the 2nd International Joint Conference on Electronic Voting* **(E-Vote-ID'17)** , October 2017.

[7] **Understanding the Mirai Botnet**
Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou
In *Proceedings of the 26th USENIX Security Symposium* **(USENIX'17)** , August 2017.

[8] **Implementing Attestable Kiosks**
Matthew Bernhard, J. Alex Halderman, and Gabe Stocco
In *Proceedings of the 14th IEEE Conference on Privacy, Security, and Trust* **(PST'16)** , December 2016.

[9] **Towards a Complete View of the Certificate Ecosystem**
Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. Alex Halderman
In *Proceedings of the ACM Internet Measurement Conference* **(IMC'16)** , November 2016.

Refereed Workshop Publications

[10] **Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits**
Kellie Ottoboni, Matthew Bernhard, J. Alex Halderman, Ronald L. Rivest, and Philip B. Stark
In *Proceedings of the 4th Annual Workshop on Advances in Secure Electronic Voting* **(Voting'19)** , February 2019.

[11] **Voting Technologies, Recount Methods and Votes in Wisconsin and Michigan in 2016**
Walter R. Mebane, Jr. and Matthew Bernhard
In *Proceedings of the 3rd Annual Workshop on Advances in Secure Electronic Voting* **(Voting'18)** , February 2019.

Selected Other Publications

[12] **The Security Challenges of Online Voting Have Not Gone Away**
Robert Cunningham, Matthew Bernhard, and J. Alex Halderman
In *IEEE Spectrum*, November 2016.

Speaking

Major Invited Talks and Keynotes

- **Recount 2016 and Student Voter Engagement**
  University of Pennsylvania Voter Engagement Week, Philadelphia, Pennsylvania, September 2019.
- **U.S. Civil Rights Commission testimony on voter registration security**
  Michigan Advisory Committee to the U.S. Commission on Civil Rights, Detroit, Michigan, April 2019.
- **Panel: Next Generation Voting Systems (moderator)**
  Election Verification Network Conference, Washington, D.C., March 2019.
- **Panel: Usability and Voter Verification (moderator)**
  Election Verification Network Conference, Washington, D.C., March 2019.
- **A Crash Course on Election Security**
  2018 DEF CON Voting Village, Las Vegas, Nevada, August 2018.
- **Panel: Do We Want a Recount or Not?**
  Election Verification Network Conference, Washington, D.C., March 2017.
- **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
  2017 RoadSec, São Paulo, Brazil, November 2017.
- **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
  33rd Chaos Communications Congress, Hamburg, Germany, December 2016.

Selected Talks

- **Cybersecurity and U.S. Elections**
  Invited speaker, RoadSec Pro, São Paulo, Brazil, November 2017; Invited speaker, Workshop on Electoral Technologies, Brasilia, Brazil, June 2017;
- **Internet Pinball: The Security and Privacy Impact of Redirects**
  Mozilla Security Research Summit, San Francisco, California, May 2019.

– **Election Security and You**
Midwest Security Workshop, Chicago, Illinois, April 2019.

– **Coercion-resistant, Receipt-free, and Paperless Voting**
Rump session at Financial Cryptography and Data Security 2019, St. Kitts, February 2019.

– **403 Forbidden: A Global View of Geoblocking**
Rump session, 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI'18), Baltimore, Maryland, August 2018.

– **A Constitutional Argument Against Burr-Feinstein**
Rump session, 25th USENIX Security Symposium (USENIX'16), Austin, Texas, August 2017.

Advising and Mentoring

Undergraduate Independent Work

– 2019: Henry Meng, Jensen Hwa, Thea Lau, Chand Rajendra-Nicolucci, Antonio Atkinson, Jeremy Wink, Kartikey Kandula
– 2020: Henry Meng, Jensen Hwa, Nakul Bajaj, Atreya Tata, Ryan Feng

Teaching

– **Graduate Student Instructor, Election Cybersecurity** *(Fall 2018)*
EECS 498, University of Michigan
Assisted with design and teaching of an undergraduate research course into election security. Lectured, wrote homework assignments, and oversaw ten undergraduate independent research projects.

– **Graduate Student Instructor, Introduction to Computer Security** *(Winter 2018)*
EECS 388, University of Michigan
Led discussion section, wrote and graded assignments, and lectured.

– **Course Operations Liaison, Securing Digital Democracy** *(2014–2018)*
Coursera (MOOC), University of Michigan
Assisted with content maintenance and day-to-day course operations for a massive, open online course about electronic voting and Internet voting technologies.

– **Teaching Assistant, Fundamentals of Parallel Programming** *(Spring 2015)*
COMP 322, Rice University
Shaped curriculum and led lab discussions for a introductory course on parallel programming featuring Java parallelism and Apache Spark

– **Teaching Assistant, Introduction to Program Design** *(Fall 2014)*
COMP 215, Rice University
Led lab discussions and wrote and reviewed assignments and exams for an introductory course on Java and Object Oriented Programming

Professional Service

Program Committee

- 30th USENIX Security Symposium (Sec'21)
- **Program co-chair**, 6th Workshop on Advances in Secure Electronic Voting (Voting'21)
- Fifth International Joint Conference on Electronic Voting (E-Vote-ID'20)
- **Program co-chair**, 5th Workshop on Advances in Secure Electronic Voting (Voting'20)

External Reviewer

- Election Law Journal
- ACM Conferences on Human Factors in Computing Systems (CHI'20)
- USENIX Security Symposium (Sec'19)
- ACM Internet Measurement Conference (IMC'18)
- ACM Conference on Computer and Communications Security (CCS'18)
- International Symposium on Research in Attacks, Intrusions, and Defenses (RAID'18)
- ACM Conference on Computer and Communications Security (CCS'17)
- Network and Distributed System Security Symposium (NDSS'17)
- IEEE Conference on Privacy, Security, and Trust (PST'16)

Broader Impact of Selected Projects

- **Implementing Better Election Security** (2018–present)
  Currently working with the State of Michigan and municipalities across the state to pilot risk-limiting audits to help secure Michigan's elections. Developed software that interfaces with voting technology to enable ballot comparison audits.
- **Fighting Weak IoT Security** (2017)
  Applied machine learning techniques to Internet measurement data to identify make and model of consumer devices that were infected by the Mirai botnet. Data has been used in ongoing legal proceedings by the Federal Trade Commission to encourage U.S. manufacturers to improve the default security of their devices.
- **2016 U.S. Presidential Election Recounts** (2016)
  Supported efforts to detect vote manipulation in the 2016 election in Michigan, Wisconsin, and Pennsylvania. While progress was hindered and in places entirely halted due to political and legal reasons, what little evidence htat was generated did not show that the 2016 Presidential election was fraudulent.

Professional Experience

- **Expert Witness** (2018–present)
  Served as an expert witness in several lawsuits opposing the use of direct-recording electronic voting machines. *Curling et al. v. Raffensperger*, *CGG v. Crittenden*, *Shelby Advocates for Valid Elections et al. v. Hargett et al.*

– **Software Engineering Consultant for VotingWorks** (June 2019–present)
Implemented risk-limiting audit math for VotingWorks' open source risk-limiting audit tool Arlo.

– **Data Science Consultant for Verified Voting** (June 2018–September 2019)
Collected and interpreted data on currently certified voting equipment in the United States to empower municipalities to make intelligent purchasing decisions. Focus on the cyber security impacts of voting technology.

– **Cryptography Intern, Cloudflare** (2017)
Developed Certificate Transparency monitoring features. Also built an SSL detector to determine what SSL settings customer sites can support, under the advising of Nick Sullivan.

– **Microsoft Research Intern** (2015)
Explored applications of trusted platform modules (TPMs) in voting through interfaces provided by Windows 10 under the advising of Josh Benaloh.